



Department of Defense INSTRUCTION

December 23, 1991
NUMBER 5240.11

ASD(C3I)

SUBJECT : Damage Assessments

References: (a) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, " March 27, 1990
(b) Executive Order 12333, "United States Intelligence Activities, " December 4, 1981
(c) DoD Directive 5240.2, "DoD Counter-intelligence, " June 6, 1983
(d) Department of Justice Memorandum, "Attorney General Guidelines for FBI Supervision for Conduct of Espionage Investigations of United States Diplomatic Missions Personnel Abroad, " April 17, 1990
(e) through (i), see enclosure 1

A. PURPOSE

This Instruction, under reference (a):

1. Establishes policy, assigns responsibilities, and prescribes procedures for the reporting, review, and analysis of comprehensive damage assessments of both the compromise of U.S. classified intelligence (sources and methods) and **nonintelligence** U.S. classified defense information resulting from espionage, as opposed to unauthorized disclosure.

2. Establishes the Department of Defense Damage Assessment Committee (**DoDDAC**).

3. Establishes a continuing, comprehensive interagency assessment of the impact of espionage cases worldwide with emphasis on U.S. and North Atlantic Treaty Organization (NATO) military capabilities and the implications for U.S. and NATO resources, plans, and arms control negotiation positions.

B. APPLICABILITY

This Instruction **applies** to the Office of the Secretary of Defense (**OSD**), the **Military** Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "the DoD Components").

c. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

D. POLICY

It is DoD policy that:

1. In accordance with **E.O.** 12333 (reference (b)) and DoD **Directive** 5240.2 (reference (c)), the DoD Components shall refer counterintelligence (**CI**) matters involving assigned military **personnel** to the concerned Military Department for appropriate investigation and disposition. The Components shall refer **CI** matters involving civilian personnel in the United States to the Federal Bureau of Investigation (FBI) and, when overseas, to the Military Department responsible for providing administrative and logistical support. The Military Departments' **CI** Agencies shall perform the necessary **CI** activities to resolve any allegations of espionage and coordinate with the FBI in accordance with the Department of Justice Memorandum (reference (d)). In accordance with DoD Instruction 5240.4 (reference (e)), all significant **CI** incidents shall be reported by the Components to the Deputy Assistant Secretary of Defense (Counterintelligence) (**DASD(CI)**), regardless of whatever Agency ultimately assumes investigative jurisdiction, and regardless of whether they involve **active** duty or retired military personnel, currently employed or retired DoD civilian personnel, or current or former DoD contractors.

2. The **DoDDAC** shall:

a. Ensure the timely dissemination of data relating to **potentially** compromised information to all affected DoD Components and other Executive Branch Agencies.

b. Review and evaluate all DoD single Component damage assessments and damage control reports.

c. Coordinate, review, and evaluate all DoD Component damage assessments conducted within the Department in which more than one DoD Component is affected by the compromise of classified information.

d. Ensure that DoD espionage information that relates to the loss or compromise of intelligence sources or methods are referred in accordance with Director of Central Intelligence Directive 3/16 (reference (f)).

3. A **DoDDAC** damage assessment review is the final step in a lineal process. It is conducted after a security review and classification review and usually follows **prosecutorial** or administrative actions.

4. Nothing in this Instruction is intended to delay or inhibit responsible DoD Components from conducting damage control actions immediately following the discovery or disclosure of espionage, or conducting damage assessments in accordance with DoD 5200.1-R (reference (g)).

5. The **DoDDAC** shall coordinate with appropriate DoD investigative agencies and legal entities before initiating action and developing or disseminating data information systems so as not to hamper or interfere with investigative, **legal**, or administrative actions or future legal remedies.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall designate the **DASD(CI)** to chair the **DoDDAC** and exercise policy formulation and oversight over the committee's activities and to implement paragraphs **E.1.a** through **E.1.d.**, below.

a. Provide notice of espionage and significant **CI** incidents, as defined in enclosure 2, affecting the Department of Defense to the **DoDDAC**.

b. Establish a formal system within the OSD for the conduct of damage assessments of information, materials, or equipment compromised through foreign espionage activity.

c. Ensure that this system within the OSD is responsive to the **DoDDAC**.

d. Provide ad hoc augmenters to **DoDDAC** subcommittees as required.

2. The Under Secretary of Defense (Acquisition); the ~~Assistant Secretary of Defense for Command, Control, Communications, and Intelligence~~; the Under Secretary of Defense for Policy; and the General Counsel of the Department of Defense each shall **designate** a senior **official** to **sit** as a member of the **DoDDAC** and provide ad hoc augmenters to **DoDDAC** subcommittees as required.

3* The Secretaries of the Military Departments; the Chairman of the **Joint** Chiefs of Staff; and the Director, National Security Agency, each shall:

a. Designate a senior official to sit as a member of the **DoDDAC** and provide ad hoc augmenters to **DoDDAC** subcommittees as required.

b. Establish a formal system within their respective Departments for the conduct of damage assessments of information, materials, or equipment compromised through foreign espionage activity.

- c. Ensure that this system is responsive to the **DoDDAC**.
- 4. The Director, Defense Intelligence Agency, shall:
 - a. Designate a senior representative to sit as a member and serve as **Executive Secretary, DoDDAC**.
 - b. Execute those functions and procedures relating to damage assessment processes delineated in sections D., above, and F., below, on behalf of the Chair, **DoDDAC**, as the Chair may direct.
 - c. Establish a formal system in the Agency for the conduct of damage assessments of information, material, or equipment **compromised** through espionage activity and ensure that this system within the Agency is responsive to the **DoDDAC**.
- 5. The Directors of Defense Agencies, other than the Defense Intelligence Agency and the National Security Agency, shall:
 - a. Establish a formal system in their Agencies for the conduct of damage assessments of information, material, or equipment compromised through espionage activity.
 - b. Ensure that the system within their Agencies is responsive to the **DoDDAC**.

F. PROCEDURES

- 1. The Chairman of the **DoDDAC** shall be the **DASD(CI)**.
- 2* The permanent **DoDDAC** membership shall include designated senior representatives appointed by the principals of the following DoD Components: Department of the Army; Department of the Navy (including a representative for the Marine Corps); Department of the Air Force; the Chairman of the Joint Chiefs of Staff; Office of the Under Secretary of Defense (Acquisition); Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; Under Secretary of Defense for Policy; National Security Agency (**NSA**); Defense Intelligence Agency (**DIA**); and the Office of the General Counsel of the Department of Defense.
- 3. The Chair, **DoDDAC**, may invite additional representatives from the Department of Defense, the FBI, and the Central Intelligence Agency to participate in committee actions on a case-by-case basis.
- 4. The representative of the Director, **DIA**, shall serve as Executive Secretary of the **DoDDAC** and shall be responsible for:
 - a. Maintenance of records and minutes of DoDDAC meetings.

b. Maintenance of security controls over information and personnel affiliated with the **DoDDAC**.

c. If required, and in coordination with DoD investigating **Agencies**, receipt and review of reports on espionage and significant **CI** matters where damage assessments were completed.

d. Receipt of espionage damage assessments and damage control reports for review by **DoDDAC** members.

e. Establishment of subcommittees, ensuring **participation** from affected DoD Components and external DoD agencies, as required, to:

(1) Conduct damage assessment analyses.

(2) Assist affected Components in the conduct of damage assessments, when requested by that Component.

(3) Assist affected Components in damage control when requested by that Component and directed by the Chair, **DoDDAC**.

(4) Make recommendations on damage assessment procedures to the **DoDDAC** membership.

(5) Coordinate, review, and evaluate damage assessments and review Component damage control actions.

(6) Provide a continuing and comprehensive aggregate assessment, coordinated with **DoDDAC** members, on the impact of the damage of foreign espionage activity worldwide on the Department of Defense.

(7) Maintain appropriate liaison with the DoD Components to facilitate the timely transmittal of data relating to the compromise of classified DoD information through espionage against allied countries.

f. **Appointment** of chairs of the subcommittees in coordination with the Chair, **DoDDAC**.

g. Establishing and maintaining a comprehensive data base that shall include a record of all damage assessments.

h. Ensuring actions **by** the **DoDDAC** are conducted in coordination with appropriate Investigating Agencies, legal entities, and affected DoD Components.

5. Individual espionage events may impact on one or multiple DoD Components. When this occurs:

a. A damage assessment shall normally be conducted by the DoD Component that was the originator of, or has proprietary interest in, the information, material, or equipment compromised by **foreign espionage activity**. The affected Component shall be **responsible** for recommending to the **DASD(CI)** changes to security **policy** based on lessons learned.

b. In cases where there are multiple DoD Components affected or where other Executive Branch, **Department**, or Agency information is also involved because of foreign espionage activity, the affected Components shall appoint a single DoD Component to be responsible for the conduct of the damage assessment with the participation of other affected parties as stated in DoD 5200.1-R (reference (g)). The affected DoD Components shall be responsible for recommending changes to security policy to the **DASD(CI)** based upon lessons learned.

6. The **DoDDAC** shall develop and recommend to the DoD Components uniform guidance to be used in the conduct of damage assessments.

7. Notification to the **DoDDAC**, through the **DASD(CI)**, of the loss of any classified information through espionage or significant **CI** incidents as defined in enclosure 2 is required immediately. Additionally, the **DoDDAC** shall be notified when a damage assessment has begun within 30 days of the start of the assessment.

8. The heads of the DoD Components conducting damage assessments shall ensure that these activities are completed and the results will be reported in writing to the Chair of the **DoDDAC** via the Executive Secretary in a timely manner.

9. The Chair, **DoDDAC**, shall ensure that the continuing assessments are provided to the Secretary of Defense and to affected DoD Component(s), as required.

10. The Chair, **DoDDAC**, shall ensure that all damage assessments are coordinated and integrated with the Department of Defense and **Department** of Justice **CI** investigative and **prosecutorial** activities.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Instruction is effective immediately. Forward one copy of implementing documents to the Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** within 120 days.



Duane P. Andrews
Assistant Secretary of Defense
(Command, Control, Communications,
and Intelligence)

Enclosures - 2

1. References
2. Definitions

REFERENCES, continued

- (e) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," June **22**, 1987
- (f) Director of Central Intelligence Directive 3/16, (Classified Title) May 1988
- (g) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1980
- (h) Public Law 96-456, "Classified Information Procedures Act," Oct 15, 1980 (94 Stat 2025) (18 **U.S.C.(1982)**)
- (i) Military Rule of Evidence 505, Manual for Courts-Martial, page II-26, 1984
- (j) Secretary of Defense Memorandum, "Strengthening Defense Intelligence", March 15, 1991

DEFINITIONS

1. Classification Review. A formal finding that information subjected to loss or compromise is (was) legally classified at the time of the compromise. The review usually includes an assessment of the probability (risk) of damage to national security resulting from disclosure of this information or material to an unauthorized person. A classification review is obtained in all national security cases and is necessary when a determination must be made on the use of classified information as trial evidence under the Classified Information Procedures Act or Military Rule of Evidence 505 (references (h) and (i)), respectively.
2. Compromise. The known or suspected exposure of classified information or material or clandestine personnel to an unauthorized person.
3. Counterintelligence (CI) Investigation. The systematic collection of information on a person or group that is, or may be, engaged in espionage or other clandestine intelligence activity, sabotage, international terrorist activities, or assassinations conducted for, or on behalf of, foreign **powers**, organizations, or persons.
4. Damage Assessment. A multidisciplinary analysis to determine the effect of a compromise of classified information on the national security. A damage assessment is normally a **long-term**, post-prosecution effort to determine in great detail the practical effects of an espionage-related compromise on operations, systems, materials, and intelligence. In special circumstances (e.g., the suspect escapes or flees U.S. jurisdiction), a damage assessment may be conducted **pre-prosecution**. The **damage** assessment is not to be confused with the classification review, normally performed in **support** of an espionage prosecution? or damage control performed mediately on the discovery or disclosure of espionage.
5. Damage Control. Those actions taken immediately by the affected Component after the discovery of a loss of classified information to minimize risk, limit damage, and/or prevent further loss.
6. Espionage. Activity designed to obtain, deliver, communicate, or transmit information relating to the national defense with the intent or reason to believe it will be used to **the injury** of the United States or to the advantage of a foreign nation.

7. **Intelligence Method.** Any process, mode of analyses, means of gathering data, or processing system or equipment used to produce intelligence.

8. **Intelligence Source.** A person or technical means that provides intelligence.

9. **Military Department Counterintelligence Agencies.** The U.S. Army counterintelligence **units**, the Naval Investigative Service Command, and the Air Force Office of Special Investigations.

10. **Security Review.** An administrative determination of whether certain Information is classified. Usually performed before publication or public release of defense information.

11. **Significant Counterintelligence (CI) Incident.** Include either of the **following**:

a. Investigation into the compromise of classified information wherein a reasonable belief has been established that the information has been made available to a foreign entity with interests inimical to the United States; or

b. Investigation of Espionage.